TERRORIST FINANCING INVESTIGATION AND PROSECUTION GUIDANCE

**DRAFT**

# Introduction and Overview

## Introduction

#### Scope

#### Objectives

#### Structure

#### Methodology

1. Terrorist financing (TF) takes many forms and exploits different vulnerabilities of the international and domestic financial systems. Though TF can be simple—for example, an individual directly providing funds to foreign terrorist organizations—TF also can be accomplished through complex and sophisticated financial schemes—for example, through the use of hawala networks and front companies, a tactic often used by Usama bin Laden and still used today by several terrorist organizations. Considering the wide range of TF activities, it is important to ensure that law-enforcement agencies and other government entities have sufficient capabilities to detect, investigate, and prosecute TF—a feat that can be accomplished through the use of lawful criminal process and other investigative and intelligence tools implemented in line with the FATF Standards, such as those contained in Recommendations 4, 5, 6, 30, and 31.

# Detection and Investigation of Terrorist Financing

1. Law-enforcement authorities rely on a range of capabilities and tools in order to effectively detect and investigate TF. One important capability is for cooperation and coordination among local, state, and federal agencies, as well as international cooperation and coordination through information sharing, consistent with the FATF Standards, such as those contained in Recommendations 2, 29 - 32, and 36 – 40. To be sure, TF often extends beyond borders and relies on countries lacking in cooperation and coordination, or ineffective and slow cooperation and coordination, to succeed in moving funds and funding terrorism organizations and operations. It is essential that financial intelligence and other information is collected, assessed, and used by law-enforcement agencies (LEAs) within different government agencies and between countries, in line with the FATF Standards, to detect and investigate instances of terrorist financing through joint analysis, co-ordinated and complementary law enforcement operations, or other forms of domestic and international cooperation.

## Leads or Sources of Information to Trigger a TF Investigation Information

1. A TF investigation can be triggered by a variety of sources, including financial intelligence from an FIU, customs service, or other agency that imposes a financial reporting requirement, as well as community reporting and open source information. In some instances, these sources may include multi-or all-source reporting, which can strengthen the initial investigation and provide additional targets for investigation.

|  |
| --- |
| Box 2.1. German case No 4In the spring of 2017, German authorities initiated an investigation based on the analysis of two complex STRs submitted by a commercial money value transfer service (MVTS). The two STRs consisted of approximately 2,000 transactions and more than 1,300 different names. Within the STRs, the reporting MVTS referred to internal analyses and press releases concerning TF-related investigations on suspects in Germany. The MVTS also provided cross-references to other STRs and public law enforcement information on individuals identified in the STR. Further analyses and investigation identified key members of a North Caucasus community in Europe, involved in a complex TF network with links to ISIL, FTFs, and the crisis in Iraq and Syria. A new CT investigation under the criminal TF statute was opened at the federal criminal police office responsible for analysing the underlying two STRs.Source: Germany |

|  |
| --- |
| Box 2.2. Belgium case No. 2• Belgium Case No. 2: In May 2019, Belgian authorities began an investigation into two Iraqi nationals (father and son), located in Belgium, who were known as members of an extensive financial and logistical network that was capable of sending money from Belgium/Europe to the last strongholds of ISIL. This investigation was initiated from an unclassified intelligence report from the Belgian civil intelligence service, which led to the disclosure of a Hawala network between Belgium and Syria/Iraq. The investigation showed that both suspects were involved in the financing of terrorism by the means of the Hawala banking system and an Iraqi Electronic Payment System, and had contacts with several family members in Belgium to transfer money on their behalf to Belgian FTFs in Syria and Iraq.Source: Belgium |

1. Financial components should be explored as a part of any terrorism investigation. Indeed, as terrorism investigations develop, law-enforcement agencies often identify the object of criminal conspiracies, or the targets of potential attacks, both of which likely required the terrorism suspects to rely on some form of financing to purchase weapons and other necessities for an attack. Therefore, investigations involving conduct that may involve terrorism should include deep dives into potential TF. What is more, TF investigations may be derived from non-financial intelligence sources involving criminal conduct that does not appear to be financial in nature.

|  |
| --- |
| Box 2.3. Swedish caseThe Swedish Security Service was informed by a partner that specific Swedish telephone-numbers had been identified in the context of ISIL related media. This initiated an intelligence operation with the main purpose to assess the information. A probable user was identified and it was established that the media used was in connection with high level ISIL members and active with regards to recruitment to ISIL. At the earliest stage there was not enough evidence to approach the suspect in a terrorism matter. There was, however, enough evidence to initiate a close cooperation with the National Police Authority, who could initiate a criminal investigation related to other crimes. Subsequent searches were conducted, leading to seizures and the identification of associated individuals. Parallel to the criminal investigation, the Security Service continued with the intelligence operation based on an “all sources approach” which also included financial investigative measures. Financial information was requested concerning the suspects and a number of money transfers of interest made through a MVTS provider. The MVTS provider was cooperative, and highlighted information that had been previously reported to the FIU regarding transactions that they could see, through their analysis, were connected to the suspects. This information confirmed transactions had been made from several suspects to the same person, who was assessed to be a probable facilitator of TF. Notably, false identities were used to register accounts at the MTVS provider and one of them was used to make some of the relevant transfers. Proving that this account had been used by the suspects was highly relevant. However, the false accounts were not identified until false Greek passports were found during a lawful house search. Ultimately, several parallel investigations were conducted at different Swedish authorities regarding different types of criminality and the relevant information was easily shared between those authorities. Through cooperation between prosecutors the information could be shared and used for investigating and prosecution. Source: Sweden |

|  |
| --- |
| Box 2.4. Irish caseThe Terrorist Financing Investigation Office (TFIO) at Special Detective Unit commenced a Terrorist Financing investigation in response to intelligence received from international policing partners. This investigation identified persons of interest, who rapidly were re-categorised as suspects in a financial facilitation network. This investigation resulted in close cooperation with the Terrorist Financing Intelligence Unit (TFIU) at Financial Intelligence Unit at Garda National Economic Crime Bureau to identify source of funds, remittance patterns and financial transaction methods. Because of intensive collaboration between TFIO and TFIU, additional persons were identified within the financial facilitation network and further analysis of financial records resulted in several STRs being generated, and the identification of remittances outside this jurisdiction by operation targets. This intelligence by TFIU, and technical examination by investigators at TFIO, led to the identification of several persons of interest being identified and additional evidence for the grounding of rearrests and searches.Source: Ireland |

## Effective Cooperation and Coordination Mechanisms

1. The cooperation and coordination of domestic government agencies is critical to countering terrorist financing. Multi-agency (sometimes referred to as the interagency) strategies are demonstrably effective in improving the detection, investigation, and prosecution of sophisticated terrorism financiers, and the use of a multi-agency strategy has proven effective for many jurisdictions in disrupting the flow of funds and other support or resources to terrorists. But the multi-agency coordination must be established before the need for an investigation arises. Indeed, agreements, authorizations, and pre-existing relationships must be in place to support a multi-agency approach to combating TF.
2. Strong interagency participation in joint investigative teams (JITs), or similar task-force-type operational bodies, in one proven way to increase multi-agency cooperation and coordination among relevant authorities. JITs lead to effective information exchange and analysis—both of which are necessary for the detection of TF activity and successful TF investigations by focusing investigative efforts (and not duplicating efforts) on TF facilitators; ensuring financial investigative techniques are used to enhance CT investigations; and monitoring threats and trends to identify possible TF transactions at their earliest point.
3. The membership of such JITs should be broad, and reflect the TF risks identified by a particular jurisdiction. For example, jurisdictions that identify the misuse of non-profit organisations (NPOs) as a specific challenge may seek to integrate NPO specialists from their NPO supervisory authority into a JIT or other operational body. Similarly, where the cross-border movement of goods is routinely used to facilitate TF, participation by customs authorities and access to trade data can be particularly important. Ensuring participation by intelligence agencies in these bodies can increase the use of lawfully collected intelligence as leads for further law-enforcement investigations.

|  |
| --- |
| Box 2.5. South Africa Counter Terrorism Functional CommitteeSouth Africa: South Africa established the Counter Terrorism Functional Committee (CTFC). All TF and CT investigations are overseen by the CTFC and conducted by Joint Teams. The permanent members of the CTFC combine their investigation in Joint Teams to investigate individual cases. The process includes the intelligence assessment, investigation and prosecution. South Africa applies a troika where intelligence, investigation and prosecution are integrated working within respective mandates.Source: South Africa |

|  |
| --- |
| Box 2.6. Israeli TF Task ForceIsrael has established a Terrorism Financing Task Force within the Israel National Police’s (INP) “Yachbal” unit. It is a trained, skilled and specialised financial investigation unit to assist in detecting TF activity. The TF Task Force includes specialists from INP, the intelligence community, the Israel Tax Authority, and the Israel Money laundering and Terror Financing Prohibition Authority. Through the Task Force, the Israeli agencies increasingly utilise financial intelligence for detection and investigation of TF cases. Source: Israel |

|  |
| --- |
| Box 2.7. U.S. Joint Terrorism Task ForcesThe United States has adopted a multi-agency strategy to cut off the flow of funds and other material support or resources to terrorists. This strategy includes the use of a Joint Terrorism Task Force (JTTF) in 104 U.S. cities, with over 4,000 personnel from over 600 state and local agencies and 50 federal agencies (including tax and customs authorities), each of which work together in coordinating investigations into terrorism, including TF. The JTTFs are made up of small teams of highly trained, locally-based, committed investigators, analysts, linguists, Special Weapons and Tactics (SWAT) experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTFs are coordinated through the interagency National Joint Terrorism Task Force (NJTTF) to ensure that information and intelligence, including information on TF trends and appropriate investigative methods to address TF, flow freely among the local JTTFs and between the local and national levels. The JTTFs work closely with federal prosecutors and the Anti-Terrorism Advisory Councils, which coordinate CT strategy and ensure information sharing among federal and local agencies.Source: United States |
| Box 2.5. 2.3. Netherlands FEC TF ProgramWithin the Netherlands, the FEC-TF Program brings together criminal, administrative and fiscal information for combating TF, and this information can be analysed in detail. The Public Prosecutor's Office is the program leader of the FEC-TF program from the point of view of the national substantive coordination role at TF. The aim of the FEC-TF Program is to enhance cooperation in the fight against terrorist financing and, more specifically, to adopt a programmatic approach to the financing and financial infrastructure of a specific terrorist organization.This program was started within the National Financial Expertise Centre (FEC), inviting not only the regular FEC-partners (prosecution service, FIU, Law enforcement agencies and regulators), but also so called participants, who are not a member of the FEC but join solely for the purpose of this TF-program. These are important organizations when it comes to TF, such as immigration and border patrol. A total of 13 government organizations are involved.The objectives of the program include mapping the financial situation of persons known to FEC partners and participants who may be associated with terrorism; developing and coordinating joint intervention strategies on the TF networks that arise (surveillance, governance, criminal investigation); and developing typologies for the financial sector and LEAs.Within the program partners exchange information, knowledge and skills. It is a joint approach: responsibilities remain with the individual organizations. Set down in a covenant. art of the program is the analysis team consisting of analysts from the FEC-TF partners and participants. This team organizes, ranks and analyzes all information exchanged by the partners and participants via the FEC unit about the TF signals transmitted. A monthly data room takes place in which signals are discussed and interventions are coordinated. This methodology is innovative and unique, not only on a national level, but also on an international level.Ultimately, the FEC-TF program allows the involved authorities to coordinate their actions on combating TF, leading to the development of the most effective disruption strategies.Source: the Netherlands |

1. Ensuring that law-enforcement authorities can access a wide variety of financial intelligence and other information from international counterparts is also crucial to effectively detecting, investigating, and prosecuting TF activity. Effective international cooperation allows for the provision of constructive and timely information and/or assistance, and LEAs and prosecuting authorities should make use of mutual legal assistance and other forms of international cooperation available to them. When competent authorities routinely seek international cooperation to pursue terrorists and their financiers, over time it helps to render the jurisdiction a less attractive location for terrorists to operate in, maintain their assets in/route their assets through, or to use as a safe haven.

|  |
| --- |
| Box 2.9. South Africa caseThis case relates to the prosecution and conviction in South Africa of a Nigerian terrorist leader for his role in orchestrating and financing two sets of bombings in the Nigerian cities of Warri and Abuja in March and October 2010. He was convicted in South Africa on terrorism, convention offences and terror financing charges and sentenced to an effective 24 years imprisonment. The first set of bombings were planned and financed by the defendant in Nigeria, but the financing and planning of the second set of bombings were conducted while the defendant was in South Africa. South African authorities became aware of his activities as a result of an information exchange between the Nigerian and South African Intelligence Agencies. A search was then conducted of the accused’s premises in South Africa, resulting in the seizure of digital and documentary evidence. The South African investigation was conducted in accordance with a multi-disciplinary approach involving the FIU, prosecution service, law enforcement and intelligence agencies. There was also close cooperation between the South African and Nigerian agencies, resulting in considerable evidence from Nigeria being obtained through an MLA process. The Nigerian government supported the prosecution by making available cooperating witnesses as well as high-ranking government officials. The financial investigations conducted by the Nigerian government were also made available to the South African authorities. The prosecution subpoenaed local banks to provide information and mobile network service providers were also subpoenaed as key communications between the accused and his accomplices were conducted by SMS. Nigerian cell phone records were also obtained through an MLA. Investigations into the text messages downloaded from the accused’s devices provided evidence as to the instructions to carry out the bombings as well as in respect of money transfers and payments, including account numbers. Evidence from co-conspirators together with sent and received text messages provided additional evidence. Source: South Africa |

|  |
| --- |
| Box 2.10. Netherlands cooperation through EurojustIn the Netherlands, the National Public Prosecution Service received some leads from Western Union and FIU-NL, indicating that FTF’s in Syria and Iraq were funded through several intermediaries in Turkey and Lebanon. The funds to those intermediaries were provided from several jurisdictions, including the Netherlands. The NPPC exchanged this information within Eurojust and organised a number of coordination meetings between the USA, Spain, France, Belgium and other countries, where information related to the case and best practices on were sharedThis approach allowed the authorities to get insight into the functioning of networks, particularly the role of intermediaries involved (those who operate between the financiers and the FTFs). In addition to the TF investigation, the authorities gathered information about offences committed by the FTFs themselves. This intelligence may be used to prosecute the FTFS after their return from the conflict zone. This international cooperation therefore provides steering information and evidence in both CT and CFT cases.Through this cooperation, several suspects have been tracked down and convicted for terrorist financing and violation of the Dutch Sanctions Act. The investigation is ongoing in the Netherlands and other countries. Source: Netherlands |

## Supporting Investigations Through Engagement with the Private Sector

1. The establishment of rapport, trust and confidence between members of LEAs and covered persons/members of the private sector can also facilitate the sharing of timely and relevant information. Meeting regularly with the private sector encourages cooperation on TF matters. Establishing good relations and having a direct point of contact between LEAs and the private sector can result in Financial Institutions and Designated non-financial businesses and professions (DNFBPs) being willing to proactively reach out to LEAs, and to quickly respond to requests for information or cooperation.

|  |
| --- |
| Box 2.11. Public Private Partnership on CFT in the NetherlandsThe Terrorist Financing Task Force (NL-TFTF) is a TF-focused co-location taskforce involving exchange of operational information and typology development. The NL-TFTF comprises four large national banks, an insurance company, FIU-NL, National Police, Fiscal Intelligence and Investigation Service and the National Prosecution Service.The NL-TFTF makes use of a general article in the Netherlands police information act, allowing sharing of investigate information with third parties only if there is a ‘pressing need’ and ‘substantial public interest’. Employing this PPP model has led to a significant increase in the quality of STR reporting. Compared to a national average of 10% of standard reporting from regulated entities (i.e. ‘unusual’ reports) meeting a threshold of FIU-designation as ‘suspicious’, 64% of NL-TFTF -responsive reporting over a 12-month period met the FIU threshold for suspicion and onward intelligence development and disclosure to law enforcement agencies.Source: the Netherlands |

|  |
| --- |
| Box 2.11. Philippines case No 2On 26 March 2016, ten (10) crew members of a tugboat, all citizens of Republic of I, were abducted off the waters of southern Philippines while on their way to a coal port in Batangas from Republic of I to Republic of P. Intelligence sources disclosed that the kidnappers were members of the Abu Sayyaf Group (ASG) who demanded Php 50,000,000.00 (approximately USD 1 million) as ransom money to be deposited to a specific bank account with National Bank of the Philippines (NBP). (The ASG, a UN-designated terrorist organization often resorts to kidnapping to fund their operations and general logistical expenses.) Authorities relied on good collaboration and coordination with NBP in order to monitor the activities of the bank account in real-time. NBP also provided timely and vital information to LEAs and intelligence agencies during the collaboration for tactical and operational purposes and in order to track movements of suspected persons and the ransom money. This close cooperation allowed for the deployment of controlled delivery techniques, and the willingness NBP to quickly provide CCTV footage of several ATM withdrawals from various NBP branches in order to establish the identity of the perpetrator(s).The intelligence and investigation reports provided by domestic counterparts, as well as the information provided by foreign counterparts, taken in conjunction with financial documents and CCTV footages acquired from NBP, were crucial in establishing the identity of the person seen withdrawing funds during the controlled delivery, as well as his association with the ASG. Based off the success of this experience, the Anti-Money Laundering Council has endeavoured to engage other covered persons, particularly money service businesses and banks, to enter into an Information-Sharing Protocol (ISP) Agreement. Source: the Philippines |

# Investigative Strategy for Specific Types of TF Threats.

1. Terrorism and its financing represent a dynamic and shifting threat stream, which requires constant adaptation by law enforcement. Just as there is no one type of terrorist, there is no one type of terrorist financier or facilitator. Furthermore, financiers and facilitators are creative, and exploit a shifting range of vulnerabilities to further their unlawful aims.
2. Some jurisdictions have identified particular threats as challenging to investigate, including the increased use of social media to solicit funds; an increase in self-radicalized individuals or small groups carrying out relatively low-cost attacks without financial support from a broader global network; and the continued use of hawala networks and the misuse of trade. Having a well-informed investigative strategy to address evolving threats should be a prerequisite for each and any TF investigation.

## The use of social media to solicit funds

1. The growth of online communication networks, including social media, has opened up new avenues for terrorists and their supporters. The ability to easily reach potential donors and connect with like-minded supporters helps to raise and move funds quickly, less transparently, and often for illicit purposes. Developing an investigative strategy for capturing and making use of online information is critical to cutting off this source of funds, and that strategy may require a multi-agency effort involving local, state, and federal law-enforcement officials.

|  |
| --- |
| Box 3.1. Argentinian case.In January 2018, an orange notification was received from Interpol reporting the existence of a micro-patronage platform designed to provide financial support, in a protected manner and anonymously, to terrorist activities that would be perpetrated in country X. Through four twitter accounts, anonymous donations for micro-patronage platforms were promoted, in crypto-currencies, in order to provide support to terrorists in country X. The operation was carried out through the use of platforms supposedly located on the dark web. Social media was an invaluable and indispensable source for gathering information on the activity that was being carried out. The investigation has relied on a mix of traditional techniques, such as searches and obtaining records (historical service, websites and protocols used during the time they were connected) and more sophisticated surveillance and information gathering (electronic devices) tools. Source: Argentina |

1. Investigations into online fundraising likely will require compelling evidence from Internet companies, such as email providers, social networking sites, and Internet Service Providers. Some providers retain records for months, others for hours, and others not at all. As a result, evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. To minimize this risk LEAs should make use of any applicable laws, where available, to direct providers to “freeze” or otherwise preserve stored records and communications. The LEAs also should seek emergency disclosure, if allowed, in the event that TF imminently will lead to death and destruction.
2. Another challenge with social media can be establishing that a particular social media account belongs to, and was used by, the defendant. Some jurisdictions have noted that the defense will often contest that a particular account was used by the defendant, instead claiming that any other person could have established a social media account using the defendant’s name or alias and a picture obtained through the internet, or that the account was altered or tampered with by another person.
3. Where applicable evidentiary rules allow, the government may be able to establish that a particular piece of evidence is authentic based on the evidence’s distinctive characteristics, such as the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, considered together with all the circumstances. Thus, prosecutors may be able to authenticate a defendant’s social media account by establishing through witness testimony and business records that the social media account was in the defendant’s name, that the account posted information that would have only been known to the defendant or his or her close associates, that the social media account was registered using email addresses or phone numbers used by the defendant, and by using other electronic evidence, such as IP log-ins, to demonstrate that the defendant was in or around a particular location when that social media account was accessed in the same area.

## Activities of “lone wolves” or small terrorist cells

1. One of the more significant shifts in terrorist activity that has occurred over the last decade is that some terrorist groups have moved away from specifically financing complex attacks and instead rely more on self-radicalized individuals or small groups who carry out relatively low-cost and unsophisticated but deadly attacks, without significant direction or support from identified terrorist operatives. Legitimate sources of funds or other assets such as income from employment, social assistance, family support, and loans are often a primary source of funding. Because these smaller groups or individuals usually do not rely on external financial or operational support, financial information about their terrorist activities may be more limited.
2. For example, as noted in the 2015 FATF Report on Emerging Terrorist Financing Risks, it is likely that the costs associated with the lethal component of the plot (e.g., obtaining assault rifle(s); explosives; funding pre-operational, out-of-country travel for training, etc.) represents the most expensive part of what may actually be a low-cost attack. Operational needs for attacks often include routine transactional activity (e.g., car rental, purchasing a hunting knife), and the financial trail associated with this activity may only involve a few personal transactions (e.g., bank-account withdrawals or credit-card charges), making it difficult to distinguish these transactions from legitimate transactions. This, in turn, can make pursuing the financial investigation appear less useful.
3. However, investigations always should include efforts to trace the money. Details associated with these transactions, to include time-and-location information, may help inform other aspects of the investigation and prove essential elements of a criminal charge in court. The investigative team also should look to whether it can prove that an identified intermediary in a transaction is a member, agent, or established conduit of a terrorist organization. If that is possible, a substantive terrorist financing charge may be available regardless of whether the ultimate end use of the funds can be identified. Otherwise, attempt, conspiracy, or the other ancillary offences set out in INR.5 may be charging options, and information returned from legal process seeking to trace the funds can often establish the substantial steps or overt acts essential to charge these inchoate offenses and lead to otherwise unidentified associates and accomplices.

|  |
| --- |
| Box 3.2. Singapore Case AIn 2016, Singapore authorities arrested a group of foreign nationals from Country B working in Singapore who had formed a clandestine group. Their aim was to overthrow Country B’s government through an armed struggle, establish an Islamic caliphate in Country B, and eventually join up with ISIS. The Commercial Affairs Department (CAD) of the Singapore Police Force, Singapore’s Counter-Terrorism Financing enforcement authority, conducted a parallel TF investigation following the arrest of the radicalised individuals, supported by various forms of information, such as oral interviews of the subjects, financial information, and social media intelligence. The investigation revealed that during their meetings within Singapore, the group leader solicited relatively small donations from members - between S$60 to S$500 (approximately US$35 to S$351) - to the group’s funds, raising a total amount of S$1,360 (approximately US$956). Members contributed monies from their own salaries, which were collected in cash during their meetings, and eventually consolidated for safe-keeping in the group treasurer’s personal bank accounts. There was no indication that they had received financial assistance from any other ISIS-related organisations or supporters. The co-mingling of the funds with legitimate income/monies presented challenges in funds tracing. It was essential for multiple interviews to be simultaneously conducted, and information to be cross-referenced with financial investigations, to ascertain the amount of illicit funds involved. Six defendants were charged for providing and/or collecting property for terrorist purposes, and successfully convicted. The funds they had raised were seized and forfeited to the State.Source: Singapore |

* *Case Example*:

## Identifying transactions committed through unregistered or unlicensed MVTS

1. Some jurisdictions have identified the use of hawala and the misuse of trade as particularly challenging to investigate. These networks operate on relationships that have excited for generations, based on long-standing relationships and trust. They may not actually transfer funds, infrequently comply with banking regulations, and otherwise fail to generate documentary proof (at least not in a way in which governments can typically access) of their illegal financial transactions. Simply, hawala networks do not operate in a manner that lends itself to record keeping, limiting the effectiveness of criminal process (i.e. subpoenas, search warrants, etc.).
2. However, certain techniques have proven helpful. Successfully investigating TF activity that moves between the regulated and unregulated financial system requires access to different types of data to help identify transactional activity that is connected. For example, while financial transfers in hawala networks may be batched together and not indicate the ultimate originator or beneficiary, communications or other electronic intercepts can be used to identify the key participants involved in a transfer. Evidence gathered from social media information may also prove helpful, by establishing connections and capturing incriminating communications surrounding otherwise seemingly legitimate transactions.

NEED: Other techniques to trace transactions conducted through unregistered or unlicensed MVTS?

Case Example(s): NEED examples linking financial activity occurring through unregistered MVTS with individual senders and recipients

## Investigating TF involving non-financial assets or economic resources

1. Following the revision of R.5 and the FATF Glossary in October 2016, funds or other assets now explicitly include economic resources, including oil and other natural resources, dividends and income accruing from assets, as well as any other assets that are not funds, but which potentially may be used to obtain funds, goods, or services. Moreover, as clarified in the 2016 FATF Guidance on Criminalising Terrorist Financing, the definition of funds or other assets goes far beyond what is commonly understood by the term funds and is not limited to only financial assets, but covers every possible kind of property, regardless of its corporeality (form), tangibility or movability, and whether they originate from legitimate or illegitimate sources. LEAs should ensure that the scope of their TF investigations extend to the full breadth of funds or assets as currently envisioned under R.5, and as set out in their national TF laws, and not limit themselves to an overly narrow interpretation of funds or other assets.

Case examples

# Overcoming Common Challenges to Prosecuting TF Cases

## Proving Intent and Knowledge

1. Challenges often arise in proving an individual charged with TF intended, or knew, that funds or other assets were going to support terrorism, terrorists, or terrorist organisations. Specifically, some jurisdictions still find it challenging to prosecute TF activity where the funds do not directly support, or were not intended to directly support, a terrorist act, or the illegal terrorist aims of a terrorist individual or organisation. This is often due to the erroneous belief that the primary TF offense requires the prosecuting authority to demonstrate that the terrorist financier (i.e., the person providing or collecting the funds or other assets) intended for, or had knowledge that, the funds would be used for a terrorist purpose.
2. In the context of Recommendation 5, however, for purpose of satisfying the *mens rea* requirement it should be sufficient to prove that the terrorist financier had the unlawful intention, or knowledge, that those funds or other assets were provided to, or collected for, a terrorist organisation or individual terrorist, without requiring a specific intent to further the illegal aims of the terrorist organisation or individual terrorist. This is what is commonly referred to by FATF as the criminalisation of TF “for any purpose.” *See* 2016 FATF Guidance on Criminalisation of Terrorist Financing for further discussion of this issue.
3. Other times, the challenge stems from an inability to prove the financier knew (or believed) the organisation or individual they provided or collected (or attempted to provide or collect) funds or other assets for was a terrorist organisation or individual terrorist. In other cases, it may be challenging to prove that the organisation or individual in question is in fact a terrorist organisation or individual terrorist, as defined by the relevant legislation, especially if the individual is not designated under national or international mechanisms and has not engaged in prior terrorist acts. Here the burden is on the prosecution to show, often through circumstantial evidence, what precisely the financier knew about the person (or organisation) and its aims.
4. In order to meet these requirements in practice, authorities may have to make use of various types of evidence. For example, it is not required that the funds or other assets ultimately reach a terrorist organisation; in the context of Recommendation 5, it is only necessary that the offender *intended* to make the funds or other assets *available* to a terrorist organisation. Short of a confession, however, proving this intent or knowledge is usually achieved through the use of other evidence, such as intercepted communications (including text messages, telephone calls and social media records), as well as the use of undercover operations, where allowed, to show that the defendant knew the organisation was a terrorist organisation. More typically, however, knowledge is established circumstantially. In some cases, the manner in which the transactions were conducted will have no legitimate explanation other than concealment, which implies an unlawful knowledge of the individual’s or organisation’s terrorist status.

|  |
| --- |
| Box 4.1. Singapore Case B:Singapore Case B: In January 2020, a Singaporean (Person I) was charged in Court by the Commercial Affairs Department (CAD) of the Singapore Police Force for terrorism financing. He was convicted on a terrorism financing charge at the end of a criminal trial and sentenced to 33 months’ imprisonment. Specifically, he was convicted for giving money to support ISIS’ propaganda efforts. Investigations established that Person I had given US$316 (equivalent to S$450) to an individual in Country A on 31 October 2014 for the publication of ISIS propaganda. The monies were self-funded and provided through a MVTS provider. The investigation showed that Person I came across a request for donation on a pro-ISIS Facebook page, which showed pro-ISIS news and articles, such as its military campaigns. After seeing the donation request, Person I informed the administrator via the Facebook messaging platform of his intention to donate to the cause. Person I subsequently received remittance details through an encrypted application. He then deleted these Facebook messages in an attempt to avoid detection. LEAs relied on various investigative techniques to develop evidence of mens rea, including: interviews to ascertain the chronology of events, the suspect’s support for terrorism ideologies, and the extent of his knowledge of the purpose these funds would be used for, and/or the identities of the intended beneficiaries; examination of Person I’s accounts on various social media platforms, to establish his support for terrorism ideology (which was useful in setting the context for his knowledge of extremism and/or terrorist groups, by virtue of the materials he read, and the messages he posted to influence others); searches of the suspect’s premises to secure evidence (including documents, handphones, and other electronic devices); analysis of financial intelligence to identify suspicious financial transactions and obtaining financial records demonstrating sources and movements of funds; and forensic analysis of seized IT equipment to extract relevant chats and information. One particularly useful piece of evidence was Person I’s admission that he had created multiple social media accounts to galvanise support for ISIS, and deleted incriminating correspondences with Person M to avoid detection by authorities. Additionally, the evidence found in Person I’s social media accounts revealed his knowledge of ISIS as a terrorist entity and his support of ISIS. The usage of multiple accounts and different monikers also effectively demonstrated his knowledge that his actions were wrong or illegal.Source: Singapore |

1. Defendants may also use “opsec” (e.g., turning off phones for meetings, etc.), and prosecutors may be able to rely on that opsec as evidence of unlawful intent. Defendants may also use coded language to refer to the organisation, a particular terrorist leader, or the purpose of the transaction. Use of code words can provide evidence of a defendant’s unlawful knowledge of an individual’s or organisation’s terrorist status, as well as evidence of a defendant’s unlawful intent. However, this may require the use of expert witnesses who can provide context for the use of words or practices that are common to terrorist groups. This might be particularly relevant for cases where the TF activity is disguised under routine person-to-person transactions.
2. In other instances where the financial activity is more complex, or is obscured by multiple intermediaries, it might be helpful to have financial experts, including experts in informal value-transfer systems, such as hawala, serve as witnesses. Complicated TF investigations and prosecutions also benefit from the use of circumstantial evidence. For example, lawful searches can identify ideologies, speeches, videos, and other terrorist propaganda in a suspect’s possession, which can help demonstrate knowledge of a particular group’s status as a terrorist organisation, or an individual’s terrorist affiliation.

|  |
| --- |
| Box 4.2. Denmark Case No. 2:Danish authorities charged ten individuals with who were suspected of collecting funds for the Kurdistan Workers Party (PKK) through a Kurdish association and a Kurdish TV-station. The main financial elements of the case were collection of funds in cash from Kurdish supporters in Europe and transporting these funds by cash courier to Denmark. In Denmark the cash was deposited into a bank account in the name of a Kurdish association and then transferred to a Belgian bank account in the name of the Kurdish TV-station. (The TV-station was a de facto media outlet for PKK.) At trial, authorities needed to demonstrate that (1) the PKK was in fact a terrorist organization; (2) the association and TV station were supporting the PKK; and (3) the defendants intended for their funds to support the PKK and not the otherwise legal activity of the TV station. To do this, authorities used statements from an analyst with the Danish Security and Intelligence Service and a non-biased expert witness to establish that PKK was a terrorist organization, and that the TV-station supported PKK. Substantial efforts were made to demonstrate for the court that PKK had been responsible for acts of terrorism. Unfortunately, proving an intent to financially support PKK and not just the TV-station was a challenge for the prosecution. Mainly because of lack of evidence, eight defendants were found to be not guilty of terrorism financing, as it could not be proven that they intended to financially support PKK. Two defendants were found guilty of financing PKK, as it could be proven in court that they had previously met with PKK leadership, which established their PKK affiliation. In a separate trial in the Danish High Court, however, the two companies behind the TV-station were fined DKK 5.000.000 each (approx. EUR 660.000) and had their broadcasting license revoked.Source: Denmark |

|  |
| --- |
| Box 4.3. Belgium Case No.8:Belgium Case No.8: A suspect (A) sent funds via Turkey to his sister and mother, who had travelled to Syria to join ISIL. A sent €300 in August 2014 and €950 in July 2015, each time to known IS money collectors. Further investigation showed that he had also sent money (between €2000 and €3000) through a Hawala banker in Belgium. A claimed he only wanted to send money to his mother, who A said lived in Turkey at the time of the transfer. A also tried to argue that the money collectors were family friends and that the money was solely intended to sustain his mother, sister and her two young children. The court decided that A knew his sister’s husband was an IS fighter, and that A knew his mother and sister had knowingly and willingly joined this terrorist group. Among other evidence, his sister’s husband was in an ISIL video claiming responsibility for the 2015 Paris terrorist attacks and his young nephews were pictured wearing clothing with the IS logo. Consequently, the court judged A could not claim that he didn’t know the money would go to a terrorist group, and his defense that he only wanted to provide for his mother and sister, and help them escape IS, was found incredulous. The court decided that the suspect’s knowledge of the destination of the funds was proven, based a) on the factual elements of the case which prove he knew his family members had joined IS, and b) on his initial denial that he had sent the money, which shows he knew this was illegal.Source: Belgium |

1. Several jurisdictions have prosecuted the family or friends of Foreign Terrorist Fighters (FTFs) who have sent funds to the FTFs overseas. As demonstrated above, one common aspect of these cases is that the suspected financiers often claim that they were unaware of the true intent of the FTF for use of the funds, or the supposedly unwitting financiers intended the funds as sustaining support, such as for food, shelter, medical care, etc. Another issue identified with regards to FTF prosecutions is proving that funds or other assets were being sent to further terrorist activity in the conflict zone rather than violence that is not linked to terrorism. Charging the family or friends of an FTF with engaging in TF may be most effective when it is clear that the suspect knew the recipient of the funds was involved in violence and also provided financial support to multiple FTFs.

|  |
| --- |
| Box 4.4. Switzerland caseSwitzerland: Swiss authorities charged the parents of a suspected foreign fighter who had been providing financial support to their son. To prove they had knowledge the funds were going to support terrorism, text messages and images from their mobile phones was used to demonstrate that they knew that their son was fighting for ISIL. The amount of funds sent was also significant and well above what their son would need for his daily survival.Source: Switzerland |

1. However, in some circumstances, criminal prosecution may not be the most appropriate disruptive measures in cases where an individual sends funds to a family member in a conflict zone. Here, it is important that such financing be *potentially* subject to criminal prosecution, but that the investigating authority exercise discretion in determining whether prosecution is most effective in disrupting TF. Administrative or other alternative measures may serve as a deterrent to future financing by a suspect without having to invest the resources necessary for a criminal prosecution. Enhanced monitoring or counter-radicalization outreach may also be another option.

|  |
| --- |
| Box 4.5. Belgium Case No. 4In this case, the aunt of a young woman who had travelled from Belgium to Syria to join ISIL (with her boyfriend). When he died in combat, she married another foreign terrorist fighter. The aunt admitted she had sent the money at the request of her family to provide financial support to her niece and children in Syria, and not to fund ISIL or another terrorist group. Belgian authorities decided not to prosecute because of the limited funds transferred (3000 EUR), the full cooperation of the suspect, and the disproportionate consequences of a conviction for a terrorism offense. Instead, prosecutors decided to close the case with a warning and probation, which is dependent on no future misconduct occurring.Source: Belgium |

1. In some cases, the question of whether the funded organisation, or individual, is in fact a terrorist organisation, or individual, is central to whether a TF offence has been committed. As noted in the 2016 FATF Guidance on Criminalising Terrorist Financing, in the context of a criminal trial, it is for courts to determine whether an organisation, or individual, should be considered to be a terrorist, based on national legal procedures, including whether the individual, or entity, has been designated by the UN pursuant to UNSCR 1267/1988 and successor resolutions, or by a competent national authority.
2. Having a declared list of designated terrorist persons and organisations can prove useful in a TF prosecution because it removes the need for the prosecution to prove that the financed person or organisation is involved in terrorism; in other words, placing an organization, or person, on a list creates a legal presumption. The fact that the person or organisation has previously been determined via an administrative process to meet the relevant definition, and has been publicly listed, should be sufficient to prove that particular element of the TF offense. In theory, it should also help with proving that the financier *knew* (or should have known) the person or organisation was a terrorist or terrorist organisation, as long as the list is made public. Of course, prosecutors may still have to prove a specific individual, not individually listed but rather alleged to be a member of a declared terrorist organisation, is in fact connected to said organisation.

|  |
| --- |
| Box 4.6. US approach to proving the financing of FTOsThe United States has adopted a list-based solution to the problem of proving whether a person or group is a terrorist or terrorist organisation for purposes of bringing a TF charge. Under this approach, the United States designates publicly those people and entities determined, via an administrative process, to be involved in terrorist enterprises and precludes individuals and entities from providing material support or resources to, or engaging in financial transactions with, such listed persons or entities. One of these lists, the Foreign Terrorist Organizations (FTO) list, includes approximately 70 foreign organisations that the United States officially considers to be terrorist groups. Under U.S. law, it is a crime for any person subject to the jurisdiction of the United States to knowingly provide to an FTO “material support or resources,” which is a phrase that is defined quite broadly. A specific intent to further the illegal aims of the FTO is not required to prove a violation of this statute. Rather, to establish mens rea the government need only allege and prove the defendant knowingly provided material support or resources to X, an FTO, knowing that X was a designated terrorist organization or that X engages or engaged in terrorist activity. It is not necessary to allege that the defendant intended to further the goals of the FTO.Source: the United States |

* Other case examples
1. A designation-based approach to TF effectively means that in many cases, instead of needing to trace donated funds to some ultimate terrorist use, or proving that a financier intended the funds to be used for such purpose, a prosecutor need only establish that the defendant engaged or attempted to engage in a financial transaction with, or otherwise provided or collected funds or other assets to or for a group or person they knew were listed, or who were acting on behalf of a listed group or individual. This is true even where the transaction or other support was not designed or intended to promote terrorism.

## Use of Sensitive Intelligence

1. Unique evidentiary issues may arise in TF cases where some of the information that exists in the case is derived from intelligence or other sensitive national-security sources. Jurisdictions have noted that using evidence derived from national-security information in court proceedings can be challenging. For example, many LEAs make use of highly sensitive, sophisticated technology in criminal investigations, in response to the widespread availability of new technologies, such as encryption. The use of such technology to search for and obtain evidence can present significant issues later on, however, especially where there is the possibility of the public disclosure of details relating to those technologies during the course of legal proceedings. Rather than risk disclosure of sensitive sources or methods, governments sometimes opt to abandon prosecution of a defendant, or drop the TF charges.
2. There are procedural processes available in some jurisdictions, however, that can help the government meet its requirements to disclose information, authenticate evidence, and present witness testimony, while also protecting sensitive material, sources, or methods. In some systems, the court must balance the competing interests of providing the terrorist offender with material relevant to the proceedings with the prejudice to national security that may result from the disclosure of that material. Other options include statutes that govern the controlled disclosure of sensitive information to judges and other trial participants. Additionally, some jurisdictions have chosen to develop a separate court system for national security legal matters, which can include terrorism and terrorist financing prosecutions. Where such statutory or other processes exist, prosecutors should familiarize themselves with them, and make use of them where appropriate.

|  |
| --- |
| Box 4.7. Australia: Public Interest Immunity Claim Although open justice is the default position for courts in Australia, any party to a proceeding including the prosecution, defence and investigative agency, may make an application for a suppression/non-publication order, and/or, a closed court order. These orders can protect the identities of witnesses and undercover operatives, as well as preventing the publication of sensitive information relating to an investigation. An investigative or intelligence agency can also claim public interest immunity in order to withhold information from production on a number of grounds, such as prejudice to national security, the protection of a person, or prejudice to Australia’s international relations. A public interest immunity claim may also be made where an investigation is ongoing. It is a matter for the court to determine whether a public interest immunity claim should be upheld, balancing the competing interests of providing the terrorist offender with material relevant to the proceedings, with the prejudice to national security that may result from the disclosure of that material. Where a public interest immunity claim is upheld, the investigative agency is not required to disclose the material that is the subject of the claim. Ultimately, the court will determine if material that is the subject of a successful claim of public interest immunity can be used as evidence in a prosecution. Where the production of such material is necessary to ensure that an accused person receives a fair trial, the Court retains the power to stay a prosecution where it is in the interests of justice to do so. Source: Australia |

|  |
| --- |
| Box 4.8. U.S.: The Classified Information Procedures ActThe U.S. relies on a statute enacted in 1980 to protect the government from “graymail” - the practice by defendants in national-security cases of forcing the government to either forgo a prosecution or risk disclosure of national security intelligence information. The Classified Information Procedures Act (CIPA) establishes a procedural mechanism to protect sensitive national-security information, including classified sources and methods, while at the same time protecting a defendant’s due-process rights. CIPA does not change the government’s discovery obligations or alter the existing rules of evidence. Rather, it sets out clear mechanisms at the pretrial, trial, and appellate stages of a case by which the court can balance the due process rights of the defendant with the right of the government to prevent disclosures of material that might jeopardize national security. Amongst other things, CIPA allows the government to make an in camera and ex parte showing to the court, which could result, inter alia, in an order allowing the withholding of certain classified information from discovery; the substitution of an unclassified summary of the relevant information contained in the classified documents; or the substitution of an unclassified statement admitting relevant facts that the classified information would tend to prove. CIPA also requires the defendant to provide written pretrial notice where he reasonably expects to disclose, or cause the disclosure of, classified information, so that the government has an opportunity to identify a substitution, or summary, that would place the defendant in substantially the same position as if he disclosed the underlying classified information. If a defendant does not comply with this notice requirement, CIPA allows the court to prevent disclosure of the information and to prohibit the defendant from examining a witness with respect to the information.Source: the United States. |

Israel:

1. In jurisdictions where the government is obligated to provide the defendant with exculpatory or other evidence, a key to successful management of the prosecutor’s discovery obligations in cases involving sensitive information is to maintain close coordination with the relevant law-enforcement agencies and any affected intelligence agency. Where such coordination is allowed, working together to address issues and planning in advance to develop strategies can help to ensure that the discovery process is handled as effectively and efficiently as possible.
2. There may be times when the government will have to rely on sensitive information to prove an element of a TF charge, or otherwise introduce such information at trial. Entering sensitive information into evidence does not alter the need to protect the information. To protect sensitive information from disclosure, a court might (1) order that only portions of an exhibit be admitted into evidence, (2) choose to excise sensitive information not relevant to the inquiry, or (3) rely on a silent-witness rule, where the classified/sensitive information is shown in public court only to the judge, the defence, the jury, and the witness. In some jurisdictions it may also be possible for the government to object to any question, or line of inquiry, that may result in the public disclosure of sensitive information during the defence examination of a witness. A court might then take suitable action to safeguard against the compromise of sensitive information, such as allowing a proffer from the parties concerning the nature of information sought and the nature of the information at risk of disclosure, before deciding whether and how to limit the line of questioning going forward.
3. Sometimes the sensitive information is not the content of a document, but rather the identity of a government witness. Jurisdictions have taken various approaches to this, but one solution is to obtain a court order allowing the witness to testify using a pseudonym, in a light disguise, or behind a screen. This requires a court to determine that national security and safety concerns outweigh a defendants’ ability to conduct unfettered cross-examination (and the court’s determination may require the government present affidavits asserting a privilege and/or identifying the harm to national security).

|  |
| --- |
| Box 4.9. South Arica: Co-conspirator WitnessesIn this case, during the trial the State led evidence of co-conspirator witnesses (cooperating witnesses). These witnesses confirmed intelligence gathered by intelligence agencies. These witnesses testified in camera and their true identities were only provided to the presiding judge and the accused’s lawyers. During the trial, and as well as in the court’s judgment these witnesses were referred to only as “X” and “Y.”Source: South Africa |

Case Example:

# Confiscation and other Types of Sanctions as Means of Disruption and Punishment

1. Confiscation is one of the most powerful tools in a prosecutor’s arsenal. Confiscation in the context of TF is often used to deprive terrorists and their financiers of the instrumentalities and the means of committing the offence. Some jurisdictions have had success confiscating assets owned or controlled by terrorists/terrorist organisations that *generate* income, as a tool for disruption. Confiscation laws can enable law enforcement to not only seize and forfeit the assets belonging to those individuals who directly plan, participate, and perpetrate TF related-crimes, but in some jurisdictions may also allow for the seizure and forfeiture of the assets of those individuals or entities who provide services or launder funds to known terrorists or terrorist organisations. Thus, confiscation can be used to disrupt and dismantle the financial infrastructure that enables terrorist organisations to survive, as well as to punish and deter would-be terrorists and their financiers.
2. However, there are challenges to effectively utilizing confiscation in TF cases. Some of these challenges are not unique to terrorism or TF cases, and can occur in investigations for non-terrorism-related activity. For example, one jurisdiction (Sweden) noted that financial intelligence, apart from suspicious transaction reports, is often vague and not very detailed. Further, FIUs are usually focused on suspicious transactions and financial flows but rarely on assets held by particular individuals or entities. These challenges can be exacerbated in terrorism or TF-related cases, where the focus is on disruption or prevention of an attack, not asset seizure. Further, the asset amounts in terrorism-related cases can often be fairly small and may only consist of personal funds or asset. This can make a potential forfeiture proceeding against a convicted terrorist or terrorist financier appear to be of limited value.
3. Nonetheless, there are numerous instances where confiscation can be used effectively. One jurisdiction (Sweden) pointed to the use of administrative orders to freeze assets at the very beginning of the criminal investigation, or in appropriate instances using administrative tools or non-conviction-based (NCB) confiscation as a substitute for criminal confiscation, whether because the criminal case would be difficult to prove or for other specific reasons. Particularly where the putative defendant is overseas, NCB can provide a powerful tool for disruption. Unlike criminal forfeiture, which is *in personam* after the defendant’s conviction, a civil forfeiture complaint is brought *in rem*, that is, against the asset. Thus, prosecutors can use NCB laws to seize and forfeit significant assets that might otherwise be used to provide support for terrorist organisations.
4. It may also be more useful to pursue confiscation in cases that are focused on terrorism financing from the beginning. In these cases, follow-on investigative measures, such as physical searches or records reviews, may identify assets that are not listed in the initial financial review, which is largely focused on transactional information.

Case Examples:

1. Another jurisdiction (USA) noted the use of a confiscation provision which expressly enables U.S. law enforcement to seize and forfeit *all* assets, *wherever* located, of *anyone* engaged in planning or perpetrating acts of terrorism—regardless of whether the property was involved in the terrorist activity or is otherwise traceable to that activity, as is required by most other confiscation laws. The provision applies in both civil and criminal cases.
2. Confiscation can also be particularly useful when targeting legal entities that may be affiliated with or supporting a terrorist organisation, or who seek to avoid their obligations under a jurisdiction’s targeted financial sanctions laws.

|  |
| --- |
| Box 5.1. Canada: NPO caseCanadian authorities identified a Canadian registered charity that was funding Harakat Al Muqawama al-Islamiya (HAMAS), a listed terrorist entity in Canada. The International Relief Fund for the Afflicted and Needy –Canada (IRFAN) was a registered Canadian charity that purported to provide aid to needy people around the world, but mostly in the Palestinian Territories. Two audits by the Canada Revenue Agency showed that IRFAN was funding organizations that were either affiliated with or controlled by HAMAS. The results of the audits were turned over to the RCMP for terrorist financing investigation. Affidavits were executed to access financial records. Open source research was conducted to confirm relationships between HAMAS and the organizations that were being funded by IRFAN. Following the investigation and successful criminal case, IRFAN’s assets were seized and forfeited to the Crown.Source: Canada |

#  Summary/Conclusion